IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

VS. **No. 17-20336**

NASSEAM ELKARRA,

Defendant.

MOTION TO SUPPRESS

COMES NOW the Defendant, Nasseam Elkarra, by and through counsel, Michael E. Scholl, and moves this Honorable Court to suppress evidence seized from Mr. Elkarra's cell phone and its derivative evidence due to violations of the Fourth and Fourteenth Amendments of the United States Constitution. Mr. Elkarra would submit that the seizure and search of his cell phone and all evidence obtained from the searches either directly or indirectly should be excluded from evidence. In support of this motion, Defendant would state as follows:

1. Mr. Elkarra was indicted in the above referenced matter for violation of 21 U.S.C. § 841 and one (1) count of criminal forfeiture.

2. Prior to the indictment, DEA Agents in Memphis and San Francisco were investigating narcotics that were being shipped from California to Tennessee. Prior to the date of January 6, 2017 there was no evidence or indication that Mr. Elkarra was involved in illegal activity. There was no probable cause or reasonable suspicion to believe that Mr. Elkarra shipped, benefitted from, or was in any way involved with the illegal trafficking of narcotics. It is believed that the only information in the possession of Agents was that Mr. Elkarra was

the cousin of Jijad Hijazi and kept frequent contact with Mr. Hijazi.

3. On January 6, 2017, Mr. Elkarra, who is a natural born United States citizen, was traveling back to San Francisco from vacation in Mexico and Cuba with a travel companion.

4. Upon entering the country, Mr. Elkarra went to the kiosk to scan his passport and answer declaration questions. Mr. Elkarra claimed two hundred and seventy dollars ($270.00) worth of items. Mr. Elkarra received a receipt with a big "X" over his information. (See attached Exhibit A - CBP Form and Boarding Pass).

5. Mr. Elkarra then went to Customs where he was questioned by Customs and Border Protection, hereinafter referred to as "CBP". The Officer stamped the receipt and sent Mr. Elkarra to what was referred to as "BGC". The CBP Agent took Mr. Elkarra from Primary Screening to Secondary Screening. CBP then did a thorough search of his baggage.

6. During this time, all other passengers, including Mr. Elkarra's travel companion, were allowed to leave.

7. After his baggage was searched, Mr. Elkarra was detained and questioned by CBP Agent Deguzman. Mr. Elkarra was asked to empty his pockets and asked if he had any devices, to which he replied just his mobile phone. At that point, the conversation was interrupted by Homeland Security Investigations (hereinafter referred to as "HSI") Agent, Tim Patterson who took Mr. Elkarra's mobile phone. Agent Patterson instructed Mr. Elkarra to have a seat on a nearby conveyor belt and advised that it would take a while before walking away with his phone.

8. Agents took the phone to another location and conducted a forensic download. Instead of a routine cursory review of Mr. Elkarra's phone, Agents used software to download

the entire contents of Mr. Elkarra's cellphone including all deleted data. This process took several hours while Mr. Elkarra sat, where Agent Patterson ordered him, on the conveyor belt in the Secondary Screening area. During this time, Mr. Elkarra was questioned about his travels. Mr. Elkarra asked several times about his cellular phone, but did not receive information as to its location.

9. After throughly searching Mr. Elkarra and his luggage over a period of time, CBP Agents cleared Mr. Elkarra. Mr. Elkarra then waited at the airport for several more hours, at which point he eventually received his phone from HSI Agents. Unbeknownst to Mr. Elkarra, HSI Agents retained the downloaded data. At this point, no probable cause or reasonable suspicion existed to search Defendant's phone. Agents' forensic downloading exceeded the scope of a "routine" search at the border.

10. Approximately two (2) weeks later, HSI Agent Kimball, who was not the seizing HSI Agent, did an in depth forensic search of the phone, noting all existing and deleted data on the phone. (See attached Exhibits B(1) and B(2) - Extraction Reports.) During the extraction, Agents over several hours reviewed all of the data of Mr. Elkarra's cell phone.

11. HSI Agents then shared this information with the DEA in San Francisco. It should be noted that no information obtained from Mr. Elkarra's cellular phone showed his involvement in the illegal distribution of drugs. In fact, the information obtained only showed Mr. Elkarra's research and due diligence in determining whether to invest in the legal cannabis business in California. There were no mentions of illegally selling, distributing, or shipping marijuana. Texts and messaging showed discussions about zoning, incorporation, attorneys and other legal entities used to determine if it would be feasible to invest in the legal cannabis

business in California. In April of 2017, Mr. Elkarra abandoned the idea of investing in the legal cannabis business. It should be further noted that the original directive from the United States Attorney's office at that time was not to pursue legal cannabis businesses.

12. Once provided with the information, Special Agent Austin Curnow provided the details of the conversations, texts and information on the phone in an affidavit for a search warrant. Agent Curnow made the affidavit appear as if he had information prior to the seizure of the phone in the form of conversations that developed probable cause for a search warrant. He detailed information in his affidavit as if it was received from independent investigation. However, the reality is that all information in the affidavit concerning conversations or activity by Mr. Elkarra was actually obtained from the illegal forensic search of the cellular phone. If this information was excluded from the affidavit, then there would be no potential basis for a warrant. Agent Curnow just repeated the information received from the forensic search of the phone to fashion a story that appeared to come from other investigations.

13. Agent Curnow then applied for a search warrant from United States District Court for the Northern District of California (See Exhibit C - Application for Search Warrant). The search warrant was obtained on February 3, 2017. Sometime after this date, the DEA took possession of the forensic data from HSI. There are no records that DEA performed any additional search after the warrant was issued. All evidence received in discovery came from the forensic search of the cellular phone on January 19, 2017.

14. On November 6, 2017, authorities used this illegally obtained information to file and receive an order for Pen Register and a Trap and Trace device along with a GPS Ping Request. In the application, the Government led the Court to believe that the information in

the application came from Mr. Elkarra's phone after the February search warrant. In fact, the information came from the forensic search of the cellular phone on January 19, 2017.

ARGUMENT AND LAW

In the case at hand, Mr. Elkarra was not arrested. His phone was taken at the border without reasonable suspicion to believe that "crime may be afoot" or that Mr. Elkarra was engaged in criminal activity as required by *Terry v. Ohio*, 392 U.S. 1, 88 S.Ct. 1868, 20 L.Ed 2d 889 (1968). While Mr. Elkarra waited several hours, HSI Agents used software to make a mirror copy of his cell phone. After two (2) weeks, they again used software to perform an exhaustive search of his cell phone without a warrant. This search went far beyond a "routine" border search and was a detailed forensic search that violated Mr. Elkarra's Fourth Amendment protections against unlawful search and seizures.

To carry out the search, the Agent used special software to download and copy all data including deleted files. They then kept a mirror or exact copy of Mr. Elkarra's phone. Agents then waited until January 19, 2017 to again use special software to analyze all of Mr. Elkarra's text messages, emails and data, including those concerning attorneys.

Border searches are allowed on a limited basis as long as they are routine. In *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), the Ninth Circuit held that reasonable suspicion is required before an investigator can undertake a forensic examination of a computer as part of a search.

First it must be determined whether there was reasonable suspicion to search Mr. Elkarra's phone at the border. In order for reasonable suspicion to exist there must be "a particularized and objective basis for suspecting the particular person stopped of criminal

activity." *United States vs. Cortez*, 449 U.S. 411 (1981). The standard can only be met when the agent can actually point to "specific and articulable facts" that indicate criminal activity "may be afoot". *Terry v. Ohio* at 21, 30. These facts must be considered with other rational inferences that can be drawn from these facts that criminal activity is occurring. This is based on the totality of the circumstances. (See *Cortez*; *United States vs. Arvizy*, 534 U.S. 266 (2002)). The Court in *United States v. Edmonds*, 240 F. 3d 55 (D.C. Cir. 2001) stated that "an investigatory stop must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity". If you look to *Cotterman*, the Court must determine whether a reasonably prudent officer would be justified in his or her belief that Mr. Elkarra was engaged in ongoing criminal activity at the time he was stopped at the airport. In Mr. Elkarra's case, there are no particularized facts to lead anyone to believe he was engaged in criminal activity at the time he was stopped at the San Francisco Airport while entering the country. The Agents used the guise of a"border search" to obtain the phone and search it without a warrant for the DEA. No agents followed or monitored Mr. Elkarra prior to or after him leaving the United States. Further, there was no information to lead authorities to believe that Mr. Elkarra conducted any illegal activity while outside the United States or while he was entering the United States. Reasonable suspicion has to be more than a hunch. CBP and HSI Agents had no evidence that anything was ongoing at the border. Therefore, no reasonable suspicion that a crime was occurring existed to allow Agents to extensively search Mr. Elkarra's phone.

The search further does not meet the requirements of the Fourth Amendment protections. The Government has a high interest in protecting the country from the entry of

unwanted persons and effects into the country at its international border. However, the search may be confined to the limits of the Fourth Amendment, especially when it is not "routine". See *United States v. Flores-Montane*, 541 U.S. 149 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985). There are few cases that deal with the warrantless searches of electronic devices at the border. The Supreme Court has given little guidance, but reasonableness seems to be the standard. *Utah v. Stuart*, 547 U.S. 398 (2006); see also *Cotterman*.

The court in *Cotterman* found that forensic searches of an imaged device was much more invasive. It compared it to a strip search and required that agents needed reasonable suspicion before conducting such a search. This was due to the fact that the forensic search was of such a comprehensive nature. These searches can access deleted data thereby requiring reasonable suspicion. See *Cotterman*, 709 F.3d at 962, 966 and 967. In the case at hand, a mirror image of the device was made over a period of hours using specialized programming. It was then analyzed by a Forensic Agent at a later date using specific software. Thus gaining access to applications and deleted data that were not accessible during a "routine" search. The question becomes, was this search routine? When the Agents made a mirror copy of the cellular phone and analyzed it another day, they provided themselves with a great deal of additional resources and time. Something they could not have the benefit of through a "routine" search at the Customs office. There have been a few District Court cases that have tackled this issue. Although they have no precedent or control over this Court, they can provide some guidance as to how other courts are analyzing these issues. (See *United States v. Kim*, 103 F. Supp. 3d 32 (Dist. Columbia 2015). The facts in the *United States v. Kim*

are extremely close to the facts here. Similarly, Agents misused their border search authority and seized a laptop for the purpose of gathering evidence in a pre-existing investigation. The Court ruled that the search was an invasion of privacy and unreasonable and suppressed all evidence seized from the laptop.

A key to this is the extensive nature to which the device can now be searched. In this situation, numerous files were extracted including banking, financial, and communications with his attorneys and business records. The court in *United States v. Saboonchi*, 990 F. Supp. 2d. 536, a Maryland District Court case that could be used for guidance stated, "it is the potentially limitless duration and scope of a forensic search of the imaged contents of a digital device that distinguishes it from a conventional search." The search of Mr. Elkarra's phone was hardly "routine" or conventional in nature.

The Supreme Court in *Riley v. California*, 134 S.Ct. 2473 (2014) has already recognized the special nature of cellular telephones and the search of these devices has significant Fourth Amendment impacts. The court in *Riley* indicated that a device such as a cellular telephone cannot be compared to an ordinary container. The *Riley* court further declined to extend its findings under *Robinson v. United States*, 414 U.S. 218 (197) to searches of cellular phones.

The analysis in this case is one governing exceptions to the warrant requirement. See *United States v. Ramsey*, 431 U.S. 606 (1977). Border searches have been likened to searches incident to arrests. At that point you must balance the Government's interest which is to prevent smuggling and import issues against the extreme invasion of privacy in the search of Mr. Elkarra's phone. In this case, the invasion of privacy was substantial. The cell phone search was extensively different than just a "routine" border search. The search of this phone

was not done as a result of any specific activity of Mr. Elkarra. Mr. Elkarra would submit that there was no suspicion of eminent or ongoing criminal activity. The search was substantially and highly invasive of Mr. Elkarra's privacy. Further, the search was so disconnected from the authority of the Government to search at the border that this search is unreasonable and violates Mr. Elkarra's Fourth Amendment rights.

The DEA essentially tried to get another agency to search the cellular phone because they did not have enough reasonable suspicion that a crime had been committed or was being committed to legally get a warrant. Instead of conducting a "routine" search of the phone, Agents did an in depth forensic search of the phone weeks later and called it a "routine" border search. They then fashioned a search warrant in a misleading way using the extracted material to appear as if there was an independent investigation into Mr. Elkarra. Not only did the search of Mr. Elkarra's phone violate his Fourth Amendment rights requiring exclusion of this evidence, but further the warrant should be stricken as violating *Frank v. Delaware*, 438 U.S. 154 (1978). This warrant was not issued with proper probable cause.

In looking at the affidavit for the search warrant, Mr. Elkarra would point to numerous paragraphs that are information taken from the illegal cellular phone search. In paragraph 16 of the search warrant, the Agent gives a misleading statement concerning Mr. Elkarra stating "recent intelligence shows that Nasseam Elkarra, Christopher Hefferman, Jijad Hijazi and Alexander Geiler have been working together to manufacture and distribute controlled substances..." The only information that this Agent had concerning Mr. Elkarra and communications with the other referenced individuals came from the illegal cell phone search in January.

Paragraph 17 is just a general assertion from the Agent and does not provide any particularized specifics. In fact, there was no information prior to the illegal search that Mr. Elkarra coordinated or provisioned funds for anything.

Paragraph 18 misleads the Court in that prior to the date of the illegal search, Agents had no information that Hefferman has been in regular contact with Mr. Elkarra. In fact, Mr. Elkarra had no contact with Hefferman in 2012 and didn't even know him at this time. Mr. Elkarra did not meet Mr. Hefferman until 2016.

Section B paragraphs 19, 20, 21, 22, 23, 24, 25 and 26 contain only information illegally and forensically taken from Mr. Elkarra's phone. It further indicates that the information was extracted on January 6, 2017. This information was further misleading. The phone was mirror copied on January 6, 2017, the actual information and data was extracted on January 19, 2017. As can be seen from these paragraphs, the extraction was more than routine.

Paragraph 27 also gets its only information concerning Mr. Elkarra from the illegal phone search. Paragraph 28 neglects to mention that Hijazi is Mr. Elkarra's family member/cousin. Paragraph 29 contradicts earlier paragraphs about package deliveries to Mr. Hefferman in that the investigation started in December 2016.

The above information was misleading and provides only information from the illegal forensic search. Pursuant to *Franks v. Delaware*, the Defendant is entitled to challenge the misleading nature of the affidavit of the search warrant. The Defendant must allege that the affidavit contained intentional or reckless misstatements or omitted facts that cause a technically true statement to be misleading. This entire affidavit is framed in such a fashion

as to make potentially true statements misleading. In fact statements in earlier paragraphs about Mr. Elkarra are false. Therefore, if the above enumerated paragraphs are stricken, the remaining paragraphs in the four corners of the warrant are not enough for probable cause to search the phone.

Further, Mr. Elkarra would submit that the Pen Register/Trap and Trace and GPS Applications and their derivative evidence should be suppressed because the applications used illegally seized evidence to obtain an order. (See Exhibits D(1) - Shelby County Criminal Court Application, D(2) - Shelby County Criminal Court Order on Application and D(3) - United Stated District Court Application and Order). The United States District Court Application and Order was prepared and executed in Memphis, Tennessee the day following the illegal search. Mr. Elkarra would submit that the "routine" border search was used by Agents to circumvent their legal obligations under the Fourth and Fourteenth Amendments of the United States Constitution.

WHEREFORE DEFENDANT PRAYS that this Honorable Court grant this motion and suppress all evidence seized from his cellular phone and any evidence obtained from its derivative use. That all seized data be permanently destroyed. That Defendant be allowed to amend this motion as necessary and for such further relief as the Court deems necessary.

Respectfully submitted:

s/ Michael E. Scholl
MICHAEL E. SCHOLL (16284)
Attorney for Defendant
200 Jefferson Avenue, Suite 1500
Memphis, Tennessee 38103
(901) 529-8500

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that a true and exact copy of the foregoing document has been served Assistant United States Attorney, Christopher E. Cotten at 167 North Main, Suite 800, Memphis, Tennessee 38103, via electronic delivery, on this the 26th day of January, 2018.

s/ Michael E. Scholl
MICHAEL E. SCHOLL